# Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective

Mohammad Momani[1], Subhash Challa[1], Khalid Aboura[1]
[1]University of Technology, Networked Sensors Technologies Lab. (NeST)
Information & Communication Technology Group
1 Broadway, Sydney 2007, Australia
mmomani@eng.uts.edu.au

**Abstract - This paper surveys the state of the art trust-based systems in Wireless Sensor Networks (WSN); it highlights the difference between Mobile ad hoc networks (MANET) and WSN and based on this observed difference (monitoring events and reporting data) a new trust model is introduced, which takes sensor reliability as a component of trust. A new definition of trust is created based on the newly introduced component of trust (sensor data) and an extension of node misbehaviour classification is also presented based on this new component of trust.**

## 1. Introduction

Wireless sensor networks (WSN) as a special type of mobile ad hoc networks (MANET) has an additional function to the traditional functions of an ad hoc network, which is monitoring events and reporting data. This observed difference is the foundation of our new approach to model trust in WSN.

Trust in WSN plays an important role in constructing the network and making the addition or deletion of sensor nodes from a network very smooth and transparent. The creation, operation, management and survival of WSN are dependent upon the cooperative and trusting nature of its nodes, therefore the trust establishment between nodes is a must.

Trust as prerequisite to secure communication between nodes, somebody might ask, How can we be sure that all nodes are trusted in order to establish a secure communication between them? There must be a new mechanism to establish trust in top of the existing mechanisms, so we introduce a new approach of establishing trust (assessing the node behaviour) using the sensor data as discussed in section 3. So our main contribution in this paper is introducing the sensor data as an additional metric (decisive component) to check the trustworthiness of a node which is to the best of our knowledge has not been addressed before.

In this paper we redefined trust in WSN based on the existing definitions and the newly introduced component of trust (sensor data) and we introduce a new trust computational model based on that. And we presented a survey on WSN trust based systems to help researchers getting a brief description of the problem and also to use it as a starting point to do a further research in the area. The rest of the paper is organised as follows: Section 2 presents our new trust definition and the properties of trust in WSN. We present all the related work done in the area in section 3. Section 4 presented modelling trust in WSN using the newly introduced component. In section 5 we introduced a new approach of trust formation and section 6 concludes the paper.

## 2. Trust definition and properties

Trust has been defined differently by researchers belong to different research communities. Even in the same research field trust can be defined in a different way depends on the application and the methodology used to calculate trust. We believe that properly defining trust in WSN is the key to understand the meaning of trust and to easily model trust, which is not yet done properly. So firstly we will try to define trust based on the trust classification discussed in [1] and the newly introduced component of trust (sensor data) as discussed later in the paper and from the definition we will be extracting the properties of trust.

Here we will use the same approach given in [1] and [2] to redefine trust with the introduction of the sensor data as a major player of defining trust. The main trust construct as discussed in [1] are: trusting behaviour, trusting intention, trusting beliefs and dispositional trust (risk). According to [2] trust can be classified into two types; reliability trust (trusting behaviour) and decision trust (trusting intention, trusting beliefs and risk). Here we are introducing sensor data as a trust component, so we are redefining trust from communication and data point of views, based on that our new definition of trust is; *Trust is the node's belief in the competence and the reliability of another node.* In other words; *Trust is the subjective probability by which node A depends on node B to fulfil its promises in performing an action and at the same time being reliable in reporting its sensor data* (here we are checking the competence of the node and its reliability and truthfulness of reporting data).

### 2.1. Properties of trust

From the above definition we can extract the following trust properties to help modelling trust efficiently.

- Trust is subjective - It is based on observations and evidence made available to the node in a specific situation.
- Trust is linked with risk - There is no reason to trust if there is no risk involved.

- Trust is intransitive - If node A trusts node B and node B trusts node C, this does not necessarily imply node A trusts node C.
- Trust is dynamic - Trust may decrease or increase by the time based on new evidence or experience.
- Trust is Asymmetric - Two nodes do not need to have similar trust in each other or about the trustworthiness of another node.
- Trust is reflexive - A node always trusts itself.

## 3. RELATED WORK

Trust in general has been the focus of many researchers for the last decade, many of them were addressing trust using different techniques to model reputation in different scenarios, mainly peer to peer networks and the internet such as in [3-7]. Trust in WSN is a new area of research and only very few people started to look at the problem such as in [1, 8-13]; however a number of people addressed some of the trust management aspects in mobile ad hoc networks (MANET), which closely resembles the WSN operation such as in [14-18]. In this section we will focus only on the work specifically addressing trust in WSN.

The authors of [8] are proposing to use a single trust value to a whole group (cluster), they are using a group trust management scheme based on their believe that sensor nodes mostly fulfil their responsibilities in a cooperative manner rather than individually. Therefore instead of calculating individual trust, it is more appropriate to calculate the trust for the entire group. This design might help saving node resources as the authors claim but it suffers from the following drawbacks, if one node is compromised (the cluster head for ex.) it will affect the whole group and also malicious nodes within the cluster will have the same trust value as the normal nodes (malicious nodes are difficult to be excluded. Trust in groups might be beneficial when the node has the choice to join a group that can bring it most benefit [3] and also when there is a high mobility in the network, which is not the case in WSN as the nodes are mainly deployed to monitor an event. In section (5) we are proposing a new approach to calculate trust, which we believe is more robust and more efficient than the suggested approach in [8] and addresses its drawbacks.

The authors of [8] are calculating the group trust in three phases, trust calculation at the node, at the cluster head and at the base station. The authors are assuming each node to have a unique ID in the group, and that is not the case in WSN as they are deployed in tens of thousands of nodes and the assignment of unique IDs is not possible and the authors are recognising that as a problem in their conclusion remarks. In their scheme [9], which is based on a distributed trust model to produce trust relationship for sensor networks, they use personal reference and reference as inputs parameters to define trust value (intention). Personal reference according to [9] consists of cryptographic operations parameters, which represent the security mechanisms and node interactive behaviour parameter, which reflects node availability. We think the scheme in [9] is very complicated especially the security part as they are assuming the communication is happening between base station and node, which is going to generate lots of traffic, (Base stations should not and can not communicate with all nodes, as the range of a node is small, instead nodes in a cluster talk to their cluster head, and cluster heads talk to a sink or a base station.

The authors of [10] were the first to introduce sensor data in their scheme as a function of the watchdog mechanism to calculate trust and according to them the web of trust embedded in every network is used to predict the behaviour of nodes in the network. In their scheme presented in [10], reputation is not a physical quantity but it is a belief; and trust is obtained by taking the statistical expectation of the probability distribution representing the reputation between the two nodes. The scheme operates on the principle of Bayesian decision theory (past behaviour of a node can be used to predict its future behaviour). In their Bayesian representation (BRSN) given in [10], they are assuming the presence of some sort of node authentication technique, which is required to achieve a trustworthy sensor network but on the other hand we argue that due to the mass deployment of sensor nodes in a WSN, it will be very difficult to authenticate nodes.

The authors of [13] are using in their proposed scheme (DRBTS) special nodes known as beacon nodes (BNs) to assist other sensor nodes (SNs) to determine their location based on a simple majority principle. They are proposing a trust system for excluding malicious BNs that provide false location information. In the proposed scheme BNs are monitoring other BNs behaviour, but what about the SNs themselves? If a sensor node is compromised, what is the solution? These questions are not addressed. They are modelling the network as an undirected graph $G = (V; E)$, with the set of vertices $V$ being the set of SNs and BNs and the set of edges $E$ being the link between them. The proposed system has some additional overhead and also requires extra memory to store the reputation tables [13].

## 4. MODELLING TRUST IN WSN

Trust modelling represents the trustworthiness of each node in the opinion of another node, thus each node associates a trust value with every other node [4], and based on that trust value a risk value required from the node to finish a job can be calculated. As illustrated in Fig. 1, node X might believe that node Y will fulfil 40% of the promises made, while node Z might believe that node Y will fulfil 50% of the promises made.

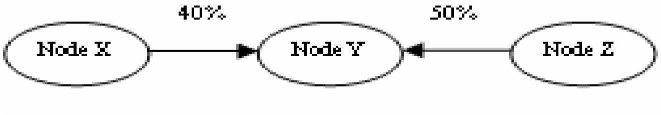

Fig. 1. A simple trust map [4]

In other words trust modelling is simply the mathematical representation of a node's opinion in another node in a network. We argue that almost all the previous work of modelling trust are approaching the problem from a communication point of view and to the best of our knowledge no one is using sensor data as a trust component other than the authors of [10], which are looking at it as a function of the watchdog mechanism, which we believe is not sufficient as the main goal of deploying a WSN is to gather and report information regarding an event, so we are treating the sensor data as a decisive component of trust as shown in Fig. 2. At the beginning the reputation will be calculated based on the direct and indirect communication with the node as discussed in our previous work in [12].

The new approach is calculating trust in a different way, the output of the reputation is coupled with the validity of the sensor data reported from that node and based on that the trust value will be calculated (the trustworthiness of a node will be determined). The sensor data reported from the node will be tested against a predefined threshold, and if the reputation value is enough to do the job (greater or equal to a threshold) and the sensor data is above or equal the predefined threshold, then the node will be considered as trustworthy otherwise a question mark will be put on the node and it will be given another chance to report data in a predetermined period of time, and so on. Detailed analysis of the data and how is it going to be tested will be in our future work.

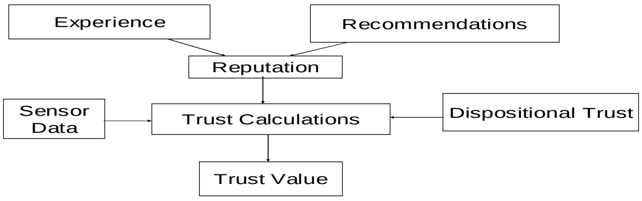

Fig. 2. Trust computational model for WSN

*4.1. Trust Formation in WSN*

Trust is calculated based on the QoS characteristics (reliability, availability, power, processing speed, memory, data rate…) the main sources for calculating trust as given in Fig. 2 are:

- Sensor Data - Data authentication, expected value
- Observation (experience) - Direct, from the node itself
- Recommendations - Indirect, from surrounding nodes
- Dispositional Trust - The risk, a node is ready to take (new node)
- Reputation (past experience) - In case no observation and experience are available

Trust formation can be divided into 3 stages, the stage of initializing trust, the stage of building trust and the stage of updating trust.

The initialization process, when the network first constructed or when a new node is introduced to the network can be in any of the following methods:
1) All nodes are considered to be trustworthy. This is the quickest method of establishing trust, but it is very risky as malicious node can be given a higher trust value. It is a practical method when the network deployment is not for a critical mission (reading temperature)
2) All nodes are considered to be untrustworthy. It is very slow method (trust formation takes very long time to be established, but on the other hand it is very robust and can be used in a critical mission networks (battlefields).
3) All nodes are neutral; they are neither trustworthy nor untrustworthy. It is in between compared to the other mentioned methods.

The building stage is the process of forming (calculating) trust from direct interactions, which can be achieved by using a watchdog mechanism as in [10] and [13] to monitor the surrounding nodes and indirect interactions (recommendations received from surrounding nodes). Most systems are using both direct and indirect interactions (positive and negative or just either one of them) to update trust, some use only direct interactions and others use only indirect information. In [10], only positive direct experience is exchanged with the surrounding nodes, while in [13], both positive and negative information is exchanged.

The evolution stage is the process of updating trust, which can be achieved using the first hand information, the second hand information or both. Most systems proposed so far use both first hand and second hand information. The main issue here is how to weight that information? Some systems give more weights to the old experience, other systems give more weight to recent experience (aging) such as in [10] and [13].

Trust values regarding other nodes should be maintained locally and updated periodically as new evidence (direct or indirect observation) becomes available. Thus, trust evolves with time as a result of evidence [5]. The evolution process can be regarded as iterating the process of trust formation as additional evidence becomes available. The level of trust must be modified as additional evidence becomes available and that will change the risk assessment of the node [6].

*4.2. Node Misbehaviour in WSN*

The main idea behind reputation and trust-based systems is to discover the misbehaving nodes and also to be very robust solutions against insider attacks (to exclude misbehaving nodes and to minimise the damage caused by inside attackers). Most of the researchers are classifying node misbehaviour from the communication point of view, however as discussed so far, WSN are deployed to sense events and report data, so we are expanding the node misbehaviour diagram given in [11] by introducing a new branch to node misbehaviour addressing sensor data (misinforming) as a new classification of node’s misbehaviour as shown below in Fig. 3.

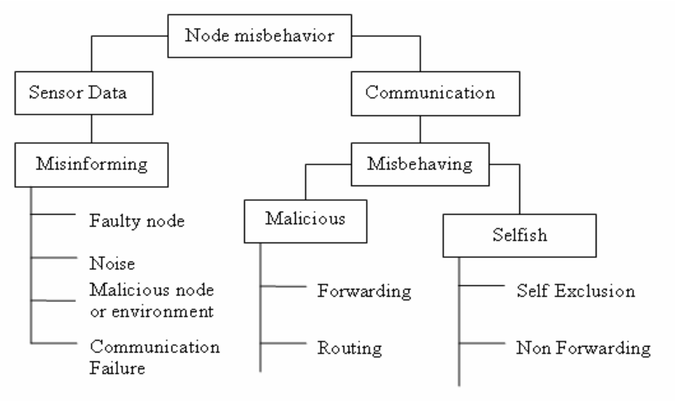

Fig. 3. Node misbehaviour classification

As can be seen from the diagram in Fig. 3, the new branch dealing with sensor data includes the misinforming behaviour of a sensor node which can be caused due to a faulty node (damaged or expired), a noise (as sensor data is not without noise), a malicious node or environment (node get captured or the environment is stuffed) or a communication failure (communication between nodes is cut off for some reason. Readers are advised to refer to [13] to get a detailed information regrading the node misbehaviour communication branch of the diagram given in Fig. 3.

## 5. A NEW APPROACH OF TRUST FORMATION

Up to this moment and to the best of our knowledge all the research been done in MANET and WSN is taking into considerations the components of trust from a communication point of view. In WSN there is more than just communication and computation, there is a sensing data, as the main goal of distributing sensor is to monitor some events and to gather some data. We argue that to the best of our knowledge we are the first researchers to address trust in WSN in terms of sensing data. We based our new approach in this section based on the existing work done by [8] with the following modifications:

Due to the massive deployment of nodes, the large area of coverage and the short communication range (distance) between nodes in WSN; nodes are grouped in a small ad hoc networks (clusters) and every node is keeping a record of only the surrounding nodes (to save resources). Each cluster has got a cluster head (reporting node) which communicates with other cluster heads or directly with the base station and off to the outside world (Internet). Here we are not giving a single trust value for each group as the authors of [8] suggested, instead we are using the default repeated small world phenomena, which means as individual nodes forms an ad hoc network between themselves, cluster heads and base stations do exactly the same with their surrounding counterparts and so on, until reaching the coverage of the whole network.

For example, as shown below in the Fig. 4; nodes A, B, C, D, E form a cluster with node R as a cluster head; nodes, F, G, H, I, J form another cluster with node S as a cluster head and nodes K, L, M, N, O forms a third cluster with node T as a cluster head. Nodes R, S and T form a cluster of cluster heads and so on, untill the convergence of the whole network; with the assumption that every node belongs to only one cluster.

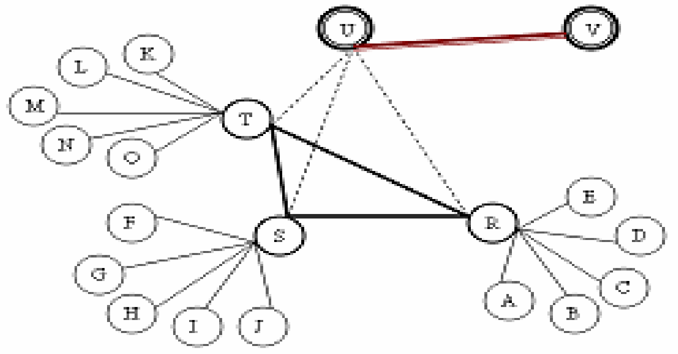

Fig. 4. A new trust model

The approach we are presenting here is different from the approach given in [8]; according to them the cluster head will aggregate all trust values for all nodes to base station and the base station will calculate the group trust value and report it back; which produces in our opinion an extra overhead on the cluster head as communication is the major resource consumer in the whole process. And as we discussed before group trust value is not recommended as the whole group can be affected in case of a cluster head get captured. Instead, in our approach we suggest that individual nodes in the cluster will have trust values for all the nodes in the cluster based on their direct and indirect interactions as shown in our previous work [12].

In addition we introduced in this approach a new trust component, which is the actual sensing data as a decisive component of node trustworthiness. We argue that, the same phenomena is valid for the cluster heads; every cluster head is keeping a record of every other cluster head in the surroundings as was the case within the cluster, and cluster heads report their trust in each other as a recommendation to the base station. The base station compares and calculates the trust in each cluster head based on the direct and indirect interactions with the cluster heads and also on the data reported from the cluster head. Following this design, we can exclude misbehaviour nodes from within the cluster at the cluster level and misbehaviour cluster heads from within the cluster heads cluster at the cluster heads level and so on till reaching the entire network level. Here we assume clusters are more powerful than normal nodes and base stations are of more power than the cluster heads. Also in our approach, we are combining the communication process and the sensor data to calculate trust not just the communication process as been the case with almost all the previous work done by all researchers to this moment.

The authors of [8] are calculating trust in three different phases to get the group trust value and in our opinion if one phase is wrong the whole result will be wrong and that is the dangerous thing about it, our scheme is calculating trust (the whole trust) at different stages (node, cluster, base station). The model suggested in [8] also does not say how to formulate trust with newly joining nodes (or what is the initial trust between nodes, just as they meet for the first time with no experience or recommendations available).

Scenario; let us consider the following design, we have deployed a network as shown in Fig. 4. where sensors are gathering the temperature of a specific area, the trust between nodes in the cluster is calculated as discussed in our work in [12]. The cluster head is periodically gathering data from all nodes in the cluster. If the data gathered from a node deviate more than a predefined threshold of the actual and estimated value, then the trust value will be affected as we will be discussing in our future work. Sensor readings are not without noise, so when we judge a reading we take into consideration the noise which can be represented as a Gaussian noise.

## 6. Conclusion and future work

In this paper we introduced a new decisive component of trust in WSN (sensor data) and based on that component we redefined trust in WSN, we introduced a new approach of modelling trust and we also introduced a new classification of nod misbehaviour in WSN. We also presented a survey on all the trusted systems in WSN. The newly presented approach is believed to be very robust as it addresses all the drawbacks from the existing approaches. In our future work we are going to select a mathematical tool to represent our trust model and simulate a network using a network simulator to verify results and finally we are planning of setting up a test bed of WSN to further verify results.

## Acknowledgement

We acknowledge funding for this research through a postgraduate scholarship from the University of Technology, Sydney and partial funding through the ARC Linkage Grant LP0561200.

## References

[1] M. Momani, J. Agbinya, G. P. Navarrete, and M. Akache, "Trust Classification in wireless sensor networks," in *8th International Symposium on DSP and Communication Systems, DSPCS'2005*. Noosa Heads, Queensland, Australia, 2005.

[2] A. Jøsang, C. Keser, and T. Dimitrakos, "Can we manage Trust?," presented at the third international conference in Trust Management, Rocquencourt, France, 2005.

[3] Y. Wang and J. Vassileva, "Bayesian Network-Based Trust Model," presented at IEEE/WIC International Conference on Web Intelligence, 2003. WI 2003., 2003.

[4] B. N. Shand, "Trust for resource control: Self-enforcing automatic rational contracts between computers," University of Cambridge Computer Laboratory UCAM-CL-TR-600, 2004.

[5] G. D. M. Serugendo, "Trust as an Interaction Mechanism for Self-Organising Systems," presented at International Conference on Complex Systems (ICCS'04), Marriott Boston Quincy, Boston, MA, USA, 2004.

[6] C. English, P. Nixon, S. Terzis, A. McGettrick, and H. Lowe, "Dynamic Trust Models for Ubiquitous Computing Environments," presented at Ubicomp2002 Security Workshop, GÖTEBORG, SWEDEN, 2002.

[7] A. Abdul-Rahman and S. Hailes, "A Distributed Trust Model," presented at Proceedings of the 1997 workshop on new security paradigms, Langdale, Cumbria, United Kingdom 1997.

[8] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y. J. Song, "Trust Management Problem in Distributed Wireless Sensor Networks," presented at 12th IEEE international conference on Embeded and Real-Time Computing Systems and Applications, 2006.

[9] Z. Yao, D. Kim, I. Lee, K. Kim, and J. Jang, "A Security Framework with Trust Management for Sensor Networks," presented at Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005.

[10] S. Ganeriwal and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," presented at the 2nd ACM workshop on Security of ad hoc and sensor networks Washington DC, USA 2004.

[11] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and Trust-based Systems for Ad Hoc and Sensor Networks," in *Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks*, A. Boukerche, Ed.: Wiley & Sons, 2007.

[12] M. Momani, J. Agbinya, R. Alhmouz, G. P. Navarrete, and M. Akache, "A New Framework of Establishing Trust in Wireless Sensor Networks," in *International Conference on Computer & Communication Engineering, (ICCCE '06)*. Kuala Lumpur, Malaysia, 2006.

[13] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed Reputation-based Beacon Trust System," in *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06)*, 2006.

[14] L. Eschenauer, "On Trust Establishment in Mobile Ad-Hoc Networks," in *Department of Electrical and Computer Engineering*, vol. Master of Science: University of Maryland, College Park, 2002, pp. 45.

[15] J. S. Baras and T. Jiang, "Dynamic and distributed trust for mobile ad-hoc networks," presented at 24th Army Science Conference, Orlando, FL, 2004.

[16] Z. Liu, A. W. Joy, and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks," presented at Distributed Computing Systems, 2004. FTDCS 2004.

[17] A. A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad-hoc Networks," presented at ACM International Conference Proceeding Series, Dunedin, New Zealand, 2004.

[18] C. R. Davis, "A localized trust management scheme for ad hoc networks," presented at 3rd International Conference on Networking (ICN'04), 2004.